İŞNET ABONELİK SÖZLEŞMESİ
DDOS ATAK ÖNLEME HİZMET EKİ

İşbu **HİZMET EKİ, İŞNET ABONELİK SÖZLEŞMESİ**'nin (bundan sonra "**SÖZLEŞME**" olarak adlandırılacaktır) ayrılmaz bir parçası olup, **SÖZLEŞME** hükümleri ile birlikte yorumlanacak ancak burada yer alan hükümlerin **SÖZLEŞME** hükümlerine aykırılık teşkil etmesi halinde, özel hüküm niteliği taşıyan işbu **HİZMET EKİ** hükümleri geçerli olacaktır.

1. TANIMLAR

İşbu **HİZMET EKİ**'nde geçen ve aşağıda belirtilmeyen ifadeler ilgili mevzuatta tanımlandıkları şekilde anlaşılacaktır. Bu maddede tekil olarak tanımlanan bir terim çoğul olarak kullanıldığında da aynı tanım çerçevesinde yorumlanır. Madde başlıkları **HİZMET EKİ**'ne sadece referans amacıyla konulmuş olup bu **HİZMET EKİ**'nin yorumlanmasını etkilemeyecektir.

Bu **HİZMET EKİ**'nde geçen tanım ve kısaltmalar aşağıdaki gibi anlaşılacaktır:

HİZMET	**İŞNET** tarafından **ABONE**'ya **HİZMET EKİ** kapsamında sunulan DDOS Atak Önleme Hizmetini,
DDOS (Dağıtık Servis Dışı Bırakma) Atak Önleme Hizmeti	**ABONE**'nin trafiğinin sürekli izlenerek bir atak durumunda **ABONE**'nin bu ataktan dolayı göreceği zararın minimuma indirgenmesini sağlamak üzere trafiğin temizlenmesinin ve temizlenen trafiğin tekrar **ABONE** lokasyonuna yönlendirilmesinin sağlandığı hizmeti,

2. KONU

İşbu **HİZMET EKİ**, İŞNET tarafından Müşteri'ye DDOS (Dağıtık Servis Dışı Bırakma) Atak Önleme Hizmeti sunulmasına ilişkin şekil ve şartlar ile **TARAF'**ların hak ve yükümlülüklerini düzenlemektedir.

3. ÖZEL HÜKÜMLER

3.1 ABONE, HİZMET'in sunulması için gereken internet bağlantısını, Statik IP adresini, ikinci bir VLAN tanımının yapılmasını ve trafiğin İŞNET güvenlik sistemlerine yönlendirilmemiş olmasını sağlamakla yükümlüdür. Bu hususların tamamının sağlanmaması nedeniyle bağlantının gerçekleştirilememesinden dolayı İŞNET sorumlu değildir.

3.2 ABONE, İŞNET'ten satın almış olduğu HİZMET'in kullanımı esnasında İŞNET ağ veya donanımlarına zarar verecek işlevlerden kaçınacak ve hizmet aldığı güvenlik sistemleri cihazlarına zarar verebilecek saldırıda vs. bulunmayacaktır. Söz konusu hallerin tespiti durumunda İŞNET HİZMET'i durdurmaya ve sözleşmeyi tek taraflı olarak haklı nedenle, tazminat ödemeksizin ve derhal feshetmeye yetkilidir.

3.3 ABONE, ağına yapılan saldırıların tespiti için kendisine ait trafik paketlerinin İŞNET Güvenlik Sistemleri tarafından açılabileceğini ve/veya başka bir cihaza yönlendirilebileceğini ve bundan dolayı İŞNET'in herhangi bir sorumluluğunun bulunmadığını kabul eder.

3.4 ABONE, İŞNET'in bilgisi dışında HİZMET üzerinde ek ve/veya değişiklik yapamaz. Bu şekilde bir ek ve/veya değişiklik yapıldığı tespit edildiğinde, sisteme zarar veren veya İŞNET tarafından kaldırılması talep edilen ek ve/veya değişiklikler kaldırılacaktır. Bu durumda, İŞNET,

yazılı bildirimiyle işbu sözleşmeyi feshetmeye ve yapılan ek ve/veya değişiklik nedeniyle uğranılan zararın tazmini için dava açmaya yetkilidir.

3.5 Hukuki düzenlemeler veya mücbir sebepler nedeniyle, HİZMET'in sunumunun durdurulması veya yetkili kurumlar tarafından HİZMET'e ilişkin teçhizatın bulunduğu yerin mühürlenmesi gibi hallerde ABONE, İŞNET'ten hiç bir hak ve tazminat talebinde bulunamaz. ABONE, Sözleşme'nin devamı süresince kendisine fatura edilen ücretleri ödemekle yükümlüdür.

3.6 Teknik olarak yeni çıkan veya sistemin tanımadığı bir saldırı tipi, virüs, trojan, worm vb. bulunursa, bunların patch'lerinin yayınlanabilmesi ve **İŞNET** güvenlik yazılımlarının bu yeni saldırıları da önleyebilmesi için **İŞNET** tarafından saldırının özelliği ve uygulamadaki durum göz önünde bulundurulduğunda, makul sayılabilecek bir zaman zarfında yapılacak gözden geçirme işlemi süresince meydana gelebilecek başta maddi ve/veya manevi ve/veya doğrudan ve/veya dolaylı zararlar olmak üzere, hiçbir zarardan **İŞNET** sorumlu değildir. Beklenmedik teknolojik gelişmelerden dolayı meydana gelebilecek başta maddi ve/veya manevi ve/veya doğrudan ve/veya dolaylı zararlar olmak üzere, hiçbir zarardan İŞNET sorumlu değildir.

3.7 HİZMET, İŞNET'in sahip olduğu teknik altyapı kapasitesi dahilinde sunulacaktır.

3.8 ABONE'nin DDOS ataklarına karşı internet trafiği koruma altında olduğu sürece bazı sitelere ve e-postalarına erişim konusunda yaşayabileceği problemlerden; e-posta sorunlarından ve yanlış alarmlardan **İŞNET** sorumlu tutulmayacaktır.

3.9 Yeni bir saldırı, virüs, trojan vs. çıkması durumunda, **İŞNET**, bu atakların engellenebilmesi için gerekli olan yama, imza vs. üretici tarafından garanti edilen süreler göz önüne alınarak, üretici tarafından gerekli güncellemeler yayınlanıncaya kadar **ABONE'**nin söz konusu ataklardan görebileceği zararlardan sorumlu tutulmayacaktır.

3.10 ABONE tarafından gerçekleştirilen konfigürasyon, kural vs. değişikliği nedeniyle güvenlik ve yama güncellemelerinin yapılamamasından **İŞNET** sorumlu tutulmayacaktır.

3.11 ABONE, yukarıda belirtilen yükümlülüklerinin yanında, yazılımları, verileri ve diğer malzemeleri üçüncü kişilerin bilgisayar sistemlerine, ağ veya donanımlarına zarar verebilecek e-maillerin gönderilmesi amacıyla kullanmayacak, zincir posta, yazılım virüsü gibi gönderilme yetkisi olmayan postaları dağıtmayacaktır.

3.12 ABONE'nin SÖZLEŞME ve HİZMET EKİ'nde belirtilen yükümlülüklerini yerine getirmemesi nedeniyle İŞNET'in hiçbir hukuki ve cezai sorumluluğu bulunmamaktadır. Bu durumda fesih için haklı neden oluşturacağı gibi, İŞNET HİZMET'i aykırılık sona erinceye kadar askıya alabilir. ABONE'nin yükümlülüklerine aykırı davranması nedeniyle ABONE, İŞNET'in uğramış olduğu/uğrayacağı tüm zararlarını karşılamakla ve ödediği tazminatı kayıtsız şartsız nakden ve defaten ödemekle yükümlüdür.

3.13 İŞNET, işbu **HİZMET**'te **ABONE**'nin bildirdiği IP Adresleri için koruma konfigürasyonu yapar. **ABONE'nin** bildirmediği IP Adresleri koruma altına alınmaz.

3.14 ABONE hizmet aldığı süreçte IP adreslerinde yaptığı/yapacağı değişiklikleri İŞNET'e bildirmelidir. Bildirmediği durumda koruma altına alınmayan trafikten dolayı İŞNET sorumlu tutulmayacaktır.

3.15 ABONE kaynaklı güvenlik zafiyetlerinden doğacak zararlardan **İŞNET** sorumlu değildir.

3.16 HİZMET yoğunluklu olarak bant genişliğini sömüren volumetrik ataklara karşı ve SSL trafik içermeyen uygulama seviyesindeki ataklara karşı DDoS Atak Önleme Sisteminin kapasitesine ve atağı tanıma yeteneğine göre koruma sağlar.

3.17 Uygulama seviyesi ataklarda daha etkin koruma sağlayabilmek üzere **ABONE**'nin kendi lokasyonunda dedike (atanmış) DDoS Cihazı konumlandırılması ayrıca tekliflendirilebilir**.**

3.18 HİZMET kapsamında sistemin başlangıçta tanıyamadığı ve/veya manuel müdahale ihtiyacı bulunan, servisin verilmesini etkileyen erişim problemlerinde ve/veya atak durumlarında, hizmet seviyesi

değerleri **İŞNET** tarafından, üreticiden gelecek cevaba göre işletilecektir. **İŞNET** belirtilen bu ve benzeri durumların gerçekleşmesi halinde 4 saat içinde çözüm önerileri üretmekle yükümlüdür**.**

3.19 ABONE'nin internet erişim hattında yaşanan ve DDoS kaynaklı olmayana problemler hizmet seviyesi değerlendirmesinin dışında tutulmaktadır.

3.20 HİZMET kapsamında **ABONE'**nin trafiği 7-14 günlük bir gözlem süresinden sonra korumaya alınabilecektir. **ABONE** talebine göre 1-4 hafta arasında değişebilen gözlem süresi de uygulanabilecektir.

3.21 Her türlü durum için DDOS ataklarının %100 engellenebileceği garantisi verilemez.

3.22 HİZMET kapsamında **ABONE**'nin sistemlere tanıtılma sürecinde, atak oluştuğunda korumaya alma evresinde ve korumadan çıkarma evresinde **ABONE'**nin almış olduğu internet hizmetinde kesintiler yaşanabilecektir. **ABONE** saldırı altında iken **HİZMET** talebinde bulunduğunda **HİZMET'**in verilmesi teknik olarak uygun görülmemektedir. Ancak atak anında devreye alma zorunluluğu oluştuğu durumda atağın kesileceği konusunda taahhüt verilmemektedir. **Atak anında ABONE'ye HİZMET verilmesi durumunda, kirli ve temiz trafiğin analiz edilemeden devreye alınması sebebi ile sorun oluşabileceği ABONE tarafından kabul edilmiş olur.**

3.23 ABONE'nin internet hizmetini aldığı devredeki IP blokları sisteme tanıtılacağından dolayı, bu IP'ler üzerinde hangi sistemlerin çalıştığı bilgisi ABONE tarafından EK-1 DDOS ATAK ÖNLEME HİZMETİ BİLGİ FORMU ile İŞNET'e iletilecektir. Bu kapsamda ABONE ilgili sunucu IP bilgilerinin (Web, Dns, Email sunucusu gibi) İŞNET ile paylaşacak olup devam eden süreçte IP bloklarında yapacağı değişiklikleri İŞNET'a bildirmelidir. ABONE, EK-1 DDOS ATAK ÖNLEME HİZMETİ BİLGİ FORMU'nda belirtilen sunucu ve IP bilgilerine göre korunacağından bu bilgileri vermekle yükümlüdür. Burada eksik olan bir bilgiden dolayı oluşan problemden İŞNET sorumlu tutulamaz.

3.24 ABONE, DDoS hizmetini etkileyebilecek değişiklikler olması durumunda EK-1 DDOS HİZMETİ BİLGİ FORMU'nu güncelleyerek iletmekle yükümlüdür. Güncellenmeyen bilgiler nedeni ile oluşan problemden İşNet sorumlu tutulamaz.

3.25 ABONE'ye sunulan HİZMET'te koruma, anında devreye girer. Sistemin yeni çıkan ya da tespit edemediği DDoS ataklarında otomatik olarak devreye girmemesi veya **ABONE'**nin haber vermesi durumunda manuel müdahale yapılabilir. Atak anında **İŞNET** güvenlik ekiplerinin incelemeleri sonucu karar vermesi durumunda Altyapı Sağlayıcı koruma noktalarına trafik yönlendirilecektir.

3.26 Inline Koruma özelliği ABONE'nin IP bloklarına ait trafiğinin sürekli olarak DDoS Atak temizleme sistemlerinden geçirilmesidir.

3.27 IP adresleri için oluşabilecek false positive durumlarından **İŞNET** sorumlu değildir.

3.28 İŞNET, atak temizleme cihazlarında oluşabilecek yoğunluk durumlarında kesinti yaşanmaması için trafiğin yönlendirmesini değiştirilebilir.

3.29 İŞNET'in HİZMET EKİ kapsamında sunduğu hizmetlere ilişkin sunduğu hizmet seviye şartları(SLA) aşağıda yer alan tabloda belirtilmektedir.

Hizmet Seviye Şartları	
Parametreler	**Değerler**
Kurulum	3 gün
Müdahale*	30 dk
Çözüm **	4 saat

** HİZMET kapsamındaki temel aksiyonların alınmasını içerir.*

***Çözüm, Abone ile karşılıklı çalışma gerektiği durumdalar hariçtir. 4 saat öngörülen çözüm süresidir.*

4. HİZMET BEDELİ

4.1 **İŞNET**'in, işbu **HİZMET EKİ** kapsamında sunacağı **HİZMET** karşılığında, **ABONE**, aşağıda yer alan tabloya göre tahakkuk edecek ücretleri ödemekle mükelleftir.

Hizmet	Miktar	Aylık Tutar (Vergiler Hariç)	KDV (%18)	Toplam Tutar (Vergiler Dahil)

** Hizmet bedeli için belirlenen süreyi ifade eder. Süre sonunda SÖZLEŞME çerçevesinde fiyatlar belirlenecektir.*

5. SÜRE

İşbu **HİZMET EKİ** imzalandığı tarihte yürürlüğe girecek olup, **SÖZLEŞME** hükümleri çerçevesinde sona erdirilinceye kadar yürürlükte kalacaktır.

SON HÜKÜM

İşbu **HİZMET EKİ** Taraflar arasında 5 (beş) maddeden ibaret olarak ……/……/…….. tarihinde **İSTANBUL**'da, bir nüshası **ABONE**'ye verilmek üzere, 2 (iki) asıl nüsha olarak imzalanmıştır.

ABONE	İŞ NET ELEKTRONİK BİLGİ ÜRETİM DAĞITIM TİCARET VE İLETİŞİM HİZMETLERİ A.Ş.
İmza: *İsim-unvan* İmza: *İsim-unvan*	İmza: *İsim-unvan* İmza: *İsim-unvan*

EK-1 DDOS ATAK ÖNLEME HİZMETİ BİLGİ FORMU

İşbu Bilgi Formu İŞNET ve ABONE arasında imzalanmış olan **SÖZLEŞME** ve **DDOS ATAK ÖNLEME HİZMET EKİ**'nin ("**HİZMET EKİ**") eki ve ayrılmaz bir parçası olup, **HİZMET EKİ** ile aynı tarihte imzalanmıştır.

ABONE				
Internet bant genişliği				
Yedek Hat Var mı?	☐ Var ☐ Yok Var ise (DDOS koruması mevcut mu)			
DDOS koruma hizmeti sağlanması istenen network bilgileri.	**IP/Subnet**			
Talep ettiğiniz DDOS öğrenme periyodu (min 1 hafta)	☐ Default (1 hafta) ☐ 2 hafta			
Atak anında koruma sağlanacak kritik sunucu ip 'leri ve verilen servisler nelerdir? Biliniyorsa bu sunucularda verilen servislerin en yüksek pps değerleri.				
DNS	**IP adres ya da adres bloğu**	**Max pps**	**DNS Türü (Cache/Authoritative)**	**TCP destekliyor mu?(Evet/Hayır)**
			A	**Evet**
HTTP (WEB)	**IP adres ya da adres bloğu**	**URL**		**Max pps**
HTTPS (WEB)	**IP adres ya da adres bloğu**	**URL**		**Max pps**
SMTP (MAIL)	**IP adres ya da adres bloğu**	**Mail domain**		**Max pps**
SIP	**IP adres ya da adres bloğu**			**Max pps**
DİĞER	**Servis**	**IP adres ya da adres bloğu**		**Max pps**
Varsa Atak gelmeyeceği düşünülen güvenilir (whitelist) ip ler	**IP adres ya da adres bloğu**			

Varsa Atak gelebileceği düşünülen engellenebilecek (blacklist) ip ler	**IP adres ya da adres bloğu**		
Diğer networklerden trafik yaratan bilinen Nat ya da Proxy adresleri	**IP adres ya da adres bloğu**		
DNS hizmeti veriliyorsa sunulan alan adları	**DNS alan adı**		**Ip adresi**
Standart olmayan portlardan verilen servisler ve port numaraları varsa belirtiniz.	**Servis**	**IP Adresi**	**Port**
TCP ,GRE, UDP, ESP, AH protokolleri ile verilen servisleriniz varsa belirtiniz.	**Servis**	**IP Adresi**	**Protokol**
Varsa verilen hizmetlerden yararlanması beklenen ülkeler.			

Yetkili Kişi Bilgileri	
Ad Soyad	
T.C. Kimlik No	
GSM No	
İş/Diğer Tel No	
E-posta	

Yukarıda sayılan bilgiler/kişisel veriler **SÖZLEŞME** ve/veya **HİZMET EKİ** kapsamında **ABONE'ye** sunulacak **HİZMET'in** ifası çerçevesinde, **HİZMET** sunulması, şifre tahsisi, ilgili kişinin kimliğinin doğrulanması, ilgili kişi ile iletişim kurulması, gerekli tanımla işlemlerinin yapılması amacı ile **İŞNET** tarafından işlenecektir.

ABONE, işbu SÖZLEŞME ve/veya HİZMET EKİ'de belirtilen hizmetlerin sunulabilmesi için İŞNET ile paylaşacağı bilgilerin 6698 sayılı Kişisel Verileri Koruma Kanunu'na ve ilgili mevzuata uygun olarak elde edilmiş olduğunu, İŞNET'e aktarılması ve İŞNET tarafından işlenmesi konusunda gerekli izinlerin alındığını, Kanun'un gerekli gördüğü hallerde ilgililerden açık ve aydınlatılmış rızanın alındığını ve bu kapsamda ilgili veri sahiplerine Kanun'un 10. maddesi kapsamında gerekli bilgilendirmelerin yapıldığını, aktarılan/paylaşılan kişisel verilerin imhasının gerekli olduğu durumlarda İŞNET'i derhal bilgilendireceğini, ABONE'nin bu hususta ki herhangi bir ihmali veya kusurlu davranışı nedeniyle İŞNET'in üçüncü bir şahıs ve/veya kurum nezdinde herhangi bir hukuki, idari ve/veya cezai taleple karşı karşıya kalması halinde, İŞNET'in tüm zararını tüm ferileriyle birlikte ödeyeceğini taahhüt eder.

ABONE